NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

Texas, North Dakota universities re-opened after bomb scares. The University of Texas at Austin allowed students back into the school's buildings September 14 after officials earlier evacuated them due to a bomb threat called in by a man who said he was linked to al Qa'ida. Minutes after the University of Texas ordered an evacuation, North Dakota State University in Fargo issued its own warning about a bomb threat and told everyone to leave its buildings. North Dakota State was also eventually re-opened after an investigation. A third school, Valparaiso University in Valparaiso, Indiana, also issued a security warning September 14. —An unspecific threat to campus was made through a graffiti message alluding to dangerous and criminal activity alleged to be carried out during the chapel break period on Friday, said a posting on its Web site. The university said it had added additional security. Source: http://www.reuters.com/article/2012/09/14/us-usa-texas-evacuation-idUSBRE88D10R20120914

Regional

(Minnesota) **Akeley water possibly contaminated.** Akeley, Minnesota residents were told not to drink city water due to possible contamination, the Park Rapids Enterprise reported September 11. A bolt on the lock at the water tower was broken September 10 and until tests were completed by the State Department of Health, residents were advised water should be used only for flushing toilets or watering lawns. The problem was expected to be resolved within 48 hours. —An unknown substance may be in the drinking water supplied by the city due to a recent break-in, the announcement being distributed throughout the city stated. Source: http://www.parkrapidsenterprise.com/event/article/id/34081/

(South Dakota) **SD salon manager dies trying to protect employee.** Police in Sioux Falls, South Dakota, said a salon manager was killed trying to protect an employee and her two children from an armed boyfriend who was upset about a domestic violence arrest and protection order. The police chief said the victim left the salon September 11 and saw the suspect in the parking lot. She phoned the store from her car to warn her employees, including the suspect's girlfriend. The victim pulled her car up to the door as the suspect stormed over. The two exchanged words then the suspect shot the victim in the head. The suspect tied up the four employees, including his girlfriend, then allowed them to leave after about 30 minutes. Armed officers stormed the salon and found the suspect dead of a self-inflicted gunshot wound. Source: http://www.seattlepi.com/news/article/Woman-killed-outside-of-SD-salon-a-sweetheart-3858214.php

National

Electromagnetic pulse could knock out U.S. power grid. U.S. power grids and other civilian infrastructure are not prepared for electromagnetic pulses (EMP) that could result from weapons or violent space weather, according to testimony at a Congressional subcommittee hearing September 12. Panelists at the House Homeland Security Subcommittee on

Cybersecurity, Infrastructure Protection, and Security Technologies, told the Chairman there were serious flaws in the nation's infrastructure that could allow for EMP events to shut down power and communications for extended periods. EMP disruptions and attacks can be triggered by various events, including high-altitude or low-altitude nuclear weapons detonations, locally based radio frequency weapons, and solar weather. One of the largest impacts from an EMP-based disruption was in Quebec, Canada in 1989, when nearly 6 million people lost power because of a geomagnetic storm. A spokesman with the Homeland Security Department's National Protection and Programs Directorate said DHS was working with federal agencies on contingency plans for an EMP event. He said the Federal Emergency Management Agency was establishing lines of communication with key agencies in case an EMP event occurs, and that the Homeland Security Secretary commissioned a report in 2011 to study the impact of space-based EMP attacks. Source: http://www.nextgov.com/defense/2012/09/electromagnetic-pulse-could-knock-out-us-power-grid/58069/

INTERNATIONAL

At least six killed in regional protests over anti-Islamic video. At least six people were reported to have been killed September 14 across the Middle East and Africa in protests over the anti-Islamic video that led to a deadly attack on a U.S. consulate in Libya. The unrest was centered mainly on U.S. embassies, but other targets also came under attack, including embassies and other outposts of Britain, Germany, and the United Nations. Three people were reported to have been killed in a violent protest near the U.S. Embassy in Khartoum, the capital of Sudan, the Arabic news service al-Arabiya reported, citing witnesses and journalists on the scene. Two people have been killed and 29 others have been injured in protests outside the U.S. Embassy in Tunis, the health ministry said. Demonstrators also set fire to the American School in Tunis, which was closed. And in Lebanon, at least one person was killed and 25 others were wounded in protests in Tripoli timed to coincide with the arrival of Pope Benedict XVI on a 3-day visit, Lebanese officials said. About 50 U.S. Marines have been sent to Yemen to provide additional security in the aftermath of the attack on the U.S. Embassy in Sanaa September 13, Defense Department officials told NBC News. The Marines, part of a Fleet Anti-Terror Security Team, were an identical unit to the one sent to Libya September 12. Source: http://worldnews.nbcnews.com/_news/2012/09/14/13856452-protests-rage-worldwide-two-reported-killed-outside-us-embassy-in-tunisia?lite

Second Belgian reactor has indications of cracks. A second nuclear reactor in Belgium has indications of cracks in its core tank, the country's nuclear regulator said September 13, putting further strain on the country's energy supply as it heads into winter. Preliminary results of tests being carried out at Tihange 2 showed that there were indications of cracks on the core tank, Belgium's nuclear regulator FANC said in a statement. The 1,008 megawatt reactor in the south of the country was to reopen from a scheduled shutdown in October, but that will now be delayed while experts analyze the test results. Source: http://www.reuters.com/article/2012/09/13/belgium-nuclear-idUSL5E8KD9D420120913

U.S. Consulate in Berlin evacuated in false alarm. German authorities evacuated part of the United States consulate in Berlin September 14 when an employee experienced breathing difficulties after handling a passport, but police said they could find no suspicious substances. Police investigators in chemical protection suits and masks searched the building but pronounced it safe for staff to return to work after several hours. An employee at the visa section had reported breathing difficulties and a metallic taste in her mouth after opening a passport handed to her by a male visitor, believed to be Albanian, police said. The alarm came amid attacks on U.S. embassy and consulate buildings across the Middle East. Source: http://www.reuters.com/article/2012/09/13/us-germany-usa-consulate-idUSBRE88C0KG20120913

Protesters attack U.S. diplomatic compounds in Egypt, Libya. The United States said it was taking measures to protect its citizens worldwide after protesters attacked U.S. diplomatic compounds in Libya and Egypt, killing four U.S. officials September 11. In Libya, witnesses said members of a radical Islamist group called Ansar al-Sharia protested near the U.S. Consulate in Benghazi and then clashed with security forces in the city, blocking roads leading to the consulate. The U.S. ambassador to Libya, a Foreign Service information management officer, and two other U.S. personnel were killed in the attack, the State Department said. In Cairo, several men scaled the walls of the U.S. Embassy and tore down its American flag. Police and army personnel formed defensive lines around the embassy in an effort to prevent demonstrators from advancing, but not before the protesters affixed a black flag atop a ladder in the American compound. Embassy officials issued a warning to Americans in Egypt, telling them to avoid the demonstrations which —may gather in front of the U.S. Embassy. The Secretary of State said that following the events the U.S. government was —working with partner countries around the world to protect our personnel, our missions and American citizens worldwide. Source: http://www.cnn.com/2012/09/11/world/meast/egpyt-us-embassy-protests/index.html

Dikes burst as rain ahead of tropical storm Leslie swamps Nova Scotia rivers. Heavy rain swamped two Nova Scotia, Canada rivers September 10, leading to flooding and evacuations in Colchester County. Two Nova Scotia rivers spilled their banks as several dikes gave way, leading to flooding that caught some residents in the Truro area by surprise. Dozens of other homes and businesses were flooded, including 40 homes on one street alone. Water levels began rising in the North and Salmon rivers near Truro, which remained under a rainfall warning as tropical storm Leslie churned toward Atlantic Canada. Source: http://www.montrealgazette.com/news/Dikes+burst+rain+ahead+tropical+storm+Leslie+swamps+Nova+Scotia/7218856/story.html

Banking and Finance Industry

Prosecutor: UBS trader accused of $2.3 billion fraud 'caused chaos,' risked bringing down bank. A senior trader at the Swiss bank UBS was a —master fraudster who lost his bank $2.3 billion, imperiling its very existence through risky deals and deceit in a bid to improve his status, bonus, and job prospects, prosecutors said September 14. A prosecution lawyer told a British

jury that the man lied to his employer, invented clients, and breached the bank's safeguards against high-risk trading between 2008 and 2011. The man was a senior equities trader with the bank in London when he was arrested in September 2011 after UBS discovered irregularities in trading records. He pleaded not guilty to two counts of fraud and two counts of false accounting. The fraud wiped $4.5 billion, or 10 percent, off the share price of Switzerland's biggest bank. Source: http://www.washingtonpost.com/business/ex-ubs-trader-goes-on-trial-accused-of-fraud-that-cost-swiss-bank-2-billion/2012/09/14/d0ed09b6-fe3b-11e1-98c6-ec0a0a93f8eb_story.html

Counterfeit bills from South America flooding US. Counterfeit money smuggled into the United States from Peru is continuing to find its way to Georgia, the Associated Press reported September 10. The bills are being smuggled from South America a year after authorities broke up a ring that flooded the Athens, Georgia area with the fake money, the Athens Banner-Herald reported. Details of the South American counterfeiting scheme were revealed when a man pleaded guilty the week of September 3 in court in Athens on a charge of possession of counterfeit currency. Peru has become the world's counterfeiting capital, the Banner-Herald reported. Peruvian counterfeiters produce about 17 percent of all fake currency circulating in the United States, authorities said. Source: http://www.sfgate.com/news/article/Counterfeit-bills-from-South-America-flooding-US-3852812.php

Visa to introduce point-to-point encryption service to payment terminals. At the end of August, Visa revealed its plans to introduce a new point-to-point encryption (P2PE) service called Visa Merchant Data Secure, Softpedia reported September 13. The service — which will be made available at the beginning of 2013 — will aim at securing payment terminals and other critical systems across the industry. The P2PE technology will allow merchants to protect sensitive cardholder information by encrypting data within the payment-processing environment. The encryption keys will be guarded by Visa, the gateway, or the firm that acquires the service. According to a member of the Visa Risk Group, the new service is not required yet, but it is a tenet of the PCI Data Security Standard. Source: http://news.softpedia.com/news/Visa-to-Introduce-Point-to-Point-Encryption-Service-to-Payment-Terminals-291895.shtml

Skimming threatens debit card users, while fraud strikes 1 percent of credit card transactions. Twice as many credit card fraud cases involve phone or online transactions than retail sales, according to new data from FICO, CardRatings.com reported September 12. However, researchers found that sophisticated counterfeit rings have raised the stakes for merchants over the most recent 20-month survey period. Researchers reported an increase in skimming. ATMs, grocery stores, and automated fuel pumps topped the list of places where criminals use stolen or cloned debit cards. According to a company spokesman, fraud rings usually test stolen cards with smaller online transactions. In a statement to reporters, he described online tests as a —relatively safe way for thieves to learn whether victims notice extra purchases on their monthly statements. The theory rings true with researchers at J.D. Power and Associates, where the results of an annual customer satisfaction survey showed that nearly a quarter of reported credit card problems involved fraudulent transactions. Source:

http://www.thestreet.com/story/11696762/1/skimming-threatens-debit-card-users-while-fraud-strikes-1-percent-of-credit-card-transactions.htm

EMV flaw allows 'pre-play' attacks on chip-enabled payment cards. Many ATMs and point-of-sale (POS) terminals fail to properly generate random numbers required by the Europay, MasterCard, and Visa (EMV) protocol to securely authenticate transaction requests, according to a team of researchers from the University of Cambridge. The use of defective random number generation algorithms make those payment devices vulnerable to so-called —pre-play attacks that allow criminals to send fraudulent transaction requests from rogue chip-enabled credit cards, the researchers said in a paper released September 11. The EMV standard requires the use of payment cards with integrated circuits capable of performing specific cryptographic functions. These cards are commonly known as chip-and-PIN cards, EMV cards, or integrated circuit cards. EMV-compliant devices must generate so-called —unpredictable numbers (UNs) for every transaction request so card issuers can verify the —freshness of these requests. Older versions of the EMV specification did not provide clear instructions for how these random numbers should be generated and only required that payment devices generate four different consecutive UNs to be compliant. The researchers found weak UN generation in devices that were easy to predict and thus take advantage of for fraudulent transactions. Source: http://www.computerworld.com/s/article/9231200/EMV_flaw_allows_pre_play_attacks_on_chip_enabled_payment_cards

Chemical and Hazardous Materials Sector

(Texas) **Halliburton hunting for missing radioactive probe in west Texas.** Halliburton Co. is scouring a 130-mile swath of west Texas oil fields for a lost 7-inch cylinder with radioactive material used when drilling natural gas wells by hydraulic fracturing, Bloomberg News reported September 13. Pickup trucks outfitted with detection gear retraced the route of a vehicle that carried the radioactive rod before it was reported missing September 11, the company told the Nuclear Regulatory Commission (NRC). The trucks drove at 10 miles an hour between Pecos, where the device was previously used on a well, and Odessa without finding the unit, said an NRC incident report. —It's not something that produces radiation in an extremely dangerous form, a spokesman for the Texas Department of State Health Services said. —But it's best for people to stay back, 20 or 25 feet if they find a cylinder marked —radioactive — do not handle, he said. The probe contains americium-241/beryllium. Source: http://www.businessweek.com/news/2012-09-13/halliburton-hunting-for-missing-radioactive-probe-in-west-texas

DHS to adopt existing terrorist screening program for chemical sites. DHS is developing a new plan for screening people with access to high-risk chemical plants for possible terrorist ties that would allow industry to make use of credentialing programs in which they already participate, agency officials said September 11. The new plan would allow chemical companies to use the existing Transportation Worker Identification Credential (TWIC) program to satisfy a DHS requirement that those with access to select facilities are screened for links to terrorist groups, the officials said. The Transportation Security Administration (TSA) and the U.S. Coast Guard

currently use the program to screen workers at port facilities and other sensitive areas. DHS pulled its previous screening proposal in July. That plan, under which chemical companies would have been required to submit information about people authorized to enter select facilities that contain toxic chemicals, was languishing at the White House Management and Budget Office since June 2011. The scrapped plan faced strong opposition from industry groups. Obtaining a TWIC credential requires people to —provide biographic and biometric information such as fingerprints, sit for a digital photograph, and successfully pass a security threat assessment conducted by the TSA, according to the agency Web site. The new plan would be submitted for White House approval and public comment by October, a DHS undersecretary told a U.S. House of Representatives subcommittee September 11. Source: http://www.nti.org/gsn/article/dhs-adopt-existing-terrorist-screening-program-chemical-sites/

Buggy malware found to target French nuclear power company. Experts have come across a malicious element in an email sent to French nuclear and energy company Areva that is misconfigured and cannot execute, Softpedia reported September 11. The email analyzed by researchers came with an executable that extracted a number of family photographs, an iTunes file, and a PDF file. While the images were likely stolen from the computer of an unwitting user, the PDF actually contained a scanned printout of an internal email from Areva-NC in Normandy, France. The information it contained was not of major importance, but it clearly showed Areva was not a random target. The malware was the Dark Comet Remote Administration Tool, one utilized on numerous occasions in malicious campaigns. However, the attack cannot cause any damage to devices because the application was not properly configured. The principal security researcher at Norman explained that the Trojan is just installed, but it is never executed. Furthermore, it is not properly configured, the overall file is very large (around 30 MB), and the iTunes file is empty and does not contain any malicious code. He believes that there are three possible scenarios: the attack is real but it does not work because the trojan is misconfigured, it may only be a test build, or it was simply meant to confuse researchers. Source: http://news.softpedia.com/news/Buggy-Malware-Found-to-Target-French-Nuclear-Power-Company-291386.shtml

NRC issues mid-cycle assessments for Nation's nuclear plants. The Nuclear Regulatory Commission (NRC) announced September 6 it has issued mid-cycle assessment letters to the nation's 104 operating commercial nuclear power plants. As of the end of June, 96 plants were in the two highest performance categories. Six nuclear reactors were in the third performance category with a degraded level of performance. For this category, regulatory oversight includes more NRC inspections, senior management attention and oversight focused on the cause of the degraded performance. These plants were: Hope Creek (New Jersey); Palisades (Michigan); Perry 1 (Ohio); Saint Lucie 1 (Florida) and Salem 1 and 2 (New Jersey). One reactor, Browns Ferry 1 in Alabama, is in the fourth performance category and requires increased oversight due to a safety finding of high significance, which will include additional inspections to confirm the plant's performance issues are being addressed. In addition to regular inspections, the NRC is currently conducting extra inspections to assess all plants' preparedness to deal with earthquakes and floods. These additional inspections are part of the NRC's post-Fukushima actions. Source: http://www.nrc.gov/reading-rm/doc-collections/news/2012/12-099.pdf

Commercial Facilities

Retail fail: Walmart, Target fared worst in Def Con social engineering contest. The third annual Def Con Social Engineering Capture the Flag Contest held at the Def Con 20 conference in July featured 20 contestants competing to elicit as much specific information, or —flags, out of employees at Walmart, AT&T, Verizon, Target, HP, Cisco, Mobil, Shell, FedEx, and UPS in cold-calls. Walmart and Target ended up with the highest scores, which means they did the worst, said a professional social engineer with social-engineer.org who lead the contest. Walmart performed the worst by exposing the most information both online and when its employees were cold-called by the social engineering contestants. Contestants posed as everything from fellow employees to office-cleaning service providers, using these phony personae as pretexts to schmooze the employees to give up seemingly benign but actually very valuable data that can expose an organization to attack. One disturbing trend: every employee who was asked to visit a URL during the call did so. Among the flags contestants could pursue were disk-encryption type, ESSID name, computer model and OS, antivirus software, name of cleaning/janitorial service, and the name of the company's third-party security guard company. Mobil and Shell employees contacted by the contestants posing as their various pretext characters were the most cautious and uncooperative in giving up information. Source: http://www.darkreading.com/insider-threat/167801100/security/attacks-breaches/240007096/retail-fail-walmart-target-fared-worst-in-def-con-social-engineering-contest.html

Communications Sector

Nothing Significant to Report

Critical Manufacturing

Nothing Significant to Report

Defense/ Industry Base Sector

(Tennessee) **Y-12 protesters mulled infiltrating New Mexico, Missouri nuclear sites: Report.** A group of three antiwar advocates targeted the Y-12 National Security Complex in Tennessee for infiltration after considering two alternative U.S. nuclear-weapon locations, and the trio used open-source information to plot the unauthorized entry over a period of months, one of the trespassers said September 12 in comments reported by the Knoxville News Sentinel. The members of the antinuclear group Transform Now Plowshares infiltrated the Oak Ridge site's —Protected Area July 28, where a facility holding large quantities of weapon-grade uranium is located. The three had enough time to allegedly pour out blood, put up signs, and paint on the sides of buildings before they were discovered and apprehended. The group's final member to be freed from detention said the group also considered attempting entry at the Los Alamos National Laboratory in New Mexico and the Kansas City Plant in Missouri. Both installations

house nuclear-weapon production facilities. Source: http://www.nti.org/gsn/article/y-12-protesters-mulled-infiltrating-new-mexico-kansas-nuclear-sites/

DOE, NNSA management faults bolster nuclear risks, auditors warn. Nuclear arms operations in the United States face greater defensive vulnerabilities and a higher potential for accidents as a result of shortcomings in how the Energy Department and the National Nuclear Security Administration oversee the private firms that manage atomic complex sites, the U.S. Government Accountability Office (GAO) said in a report published September 12. The Energy Department has moved to strengthen efforts against potential atomic mishaps in response to both historical and newer hazardous events, but personnel at scientific facilities and elsewhere have suggested the management initiatives are overextended and unnecessarily meddlesome, auditors wrote in the document. The department responded by scaling back internal rules, but Congressional investigators in April said the effort's achievements were uncertain due to a failure to assess the degree to which older rules had interfered with activities, the GAO officials said. Source: http://www.nti.org/gsn/article/nnsa-management-faults-bolster-risks-auditors-say/

Page: Critical limited edition malware targets defense industry. Researchers analyzed a piece of malware called Page. They found the critical limited edition malware is masqueraded as a PDF file and sent out to companies in the aviation defense industry. When victims open the apparently innocent PDF file, they are presented with an invitation to an upcoming industry event. While the user views the invitation, a vulnerability in collab.hetlcon() is exploited to create and execute a file. Once it is executed, the file drops a DLL, which opens a backdoor at TCP port 49163 and initiates network communications, Fire Eye experts explained. Source: http://news.softpedia.com/news/Page-Critical-Limited-Edition-Malware-Targets-Defense-Industry-291955.shtml

(Pennsylvania) **Part of Boeing's Ridley Park factory evacuated.** The part of a Boeing factory near Philadelphia that produces the CH-47 Chinook helicopter was evacuated September 11 after a threatening note was found, a company spokesman said. The note forced several hundred employees to leave the sprawling plant between 7:30 a.m. and 8:30 a.m. —The threat related to one of our production facilities, said a Boeing spokesman. The Ridley Park factory also produces the V-22 Osprey. Another spokesman said first-shift workers were sent home, but Boeing was hopeful second-shift workers would be on the job in the afternoon. —The investigation into the threat is still continuing inside the building, he said. Source: http://seattletimes.com/html/boeingaerospace/2019123113_boeingridleyxml.html

Emergency Services

Law enforcement can become go-to targets for terrorists, bulletin warns. Violent homegrown extremists see U.S. law enforcement officers as targets in the face of tougher security at more fortified locations and have access to publicly available information to help them circumvent counter-terror tactics protecting officers, according to an unclassified bulletin by the National Counterterrorism Center (NCTC), Government Security News reported September 14. The

bulletin was disseminated August 2, and said law enforcement entities are being identified by —homegrown violent extremists (HVEs) as strategic targets and targets of opportunity. The bulletin was posted on the Public Intelligence information site September 12, and stated the tactics used by undercover operations and other law enforcement to track domestic terror groups has created a feeling among a —core element of HVEs that sees such operations as persecution, reflecting an —inherent aggression towards Islam . Law enforcement has used information and undercover operations to disrupt a —a number of high-profile plots since 2009, it said. It warned that public disclosure of law-enforcement operations in the media and in publicly available court documents can lead to officers being targets of plots. Source: http://www.gsnmagazine.com/node/27277?c=law_enforcement_first_responders

(Utah) **Police badges, guns, jewelry stolen from Alpine home.** Several items were stolen from a home in Alpine, Utah, belonging to the Lone Peak Police Department, KTVX 4 Salt Lake City reported September 10. Among the missing items are several guns and police badges that were contained inside a safe that was taken from the home of a Lone Peak police officer August 28. The burglars fled when they saw the officer outside of the house. A Lone Peak police lieutenant said the safe contained 4-5 rifles, including an AR-15 rifle, a .22 caliber rifle, and a shotgun. The safe also contained knives and 4-5 handguns, including a .40 caliber pistol, a .357 Magnum, and a .45 —Glock -type gun. Source: http://www.abc4.com/content/news/top_stories/story/Police-badges-guns-jewelry-stolen-from-Alpine-home/c4iNu2MHk0-S2fLHNn-Y7A.cspx?hpt=ju_bn6

ENERGY

(California) **Feds: Pipe wall in refinery fire was thin as penny.** A corroded pipe that failed and triggered a leak and massive fire at one of California's largest refineries had walls as thin as a penny in some areas, federal investigators said. U.S. Chemical Safety Board (CSB) officials said September 12 that a key part of their probe into the fire at the plant in Richmond is why Chevron Corp. did not replace the pipe during a routine inspection a year ago. The board previously found Chevron inspected and replaced a larger, corroded 12-inch pipe connected to the smaller one that failed August 6. —We have obtained internal Chevron policies that recommend that every segment of pipe in this service should have been included in the pipe inspection program, said the lead investigator for the CSB. —There is no indication that this segment of pipe was inspected for thickness during the most recent inspections. The blaze at the San Francisco Bay area facility knocked an important refinery unit offline, reducing production. Gas prices on the West Coast have surpassed $4 a gallon since the fire. In addition, smoke from the blaze sent thousands of residents to hospitals with health complaints. Source: http://www.businessweek.com/ap/2012-09-12/feds-pipe-wall-in-refinery-fire-was-thin-as-penny

(Texas) **40,000 worth of equipment stolen in ETX oil field theft.** Harrison County, Texas officials asked for the public's help in solving an east Texas oil field theft, KFXK 51 Longview reported September 10. Authorities said a 16-foot heavy duty trailer, a control panel, and copper wiring were stolen from a Howell Oil Company well site. Howell officials claim they left the equipment

parked near Owens Corner Road. When the work superintendent returned to the location 2 days later, he found the trailer had disappeared. The tan trailer contained about 2,000 feet of heavy copper wire and a —soft-start control panel. The items were estimated to be worth $40,000. The control panel is tan and grey in color. The trailer is a heavy-duty, double-axle trailer and is also tan. The copper wire is in 200 foot and 83 foot sections. Details surrounding how the theft happened were unclear, however it appeared that the burglars may have entered the site through an unlocked gate. Source: http://www.fox51.com/news/40000-worth-equipment-stolen-etx-oil-field-theft

(South Carolina) **Marlboro Electric reports copper thefts in Dillon County.** Copper thieves struck three of Marlboro Electric's substations in Dillon County, South Carolina, in August, causing more than $23,000 in damages. The electric company said each incident resulted in a dangerous situation that could have caused an employee to be electrocuted or severely injured had they entered the substations and not noticed the vandalism. The Dillon Industrial, Moccasin Bluff, and Little Rock substations were vandalized. A spokesman said before all of the repairs were complete from the first incident, the Dillon Industrial substation was vandalized again with copper stolen. At all four crime scenes, fences were cut, ground wires were cut and left dangerously exposed, equipment was damaged, and copper wire was stolen. Source: http://www.carolinalive.com/news/story.aspx?id=798197#.UE4Sxq5ozg2

(Michigan) **Marathon Detroit refinery said to have released unknown chemical: NRC.** Marathon Petroleum Corp's 106,000 barrel-per-day refinery in Detroit is reported to have released an unknown chemical into the atmosphere September 8, according to an unidentified caller cited in a filing with national pollution regulators. "The material is causing nausea, burning eyes, and difficulty breathing to local residents," the filing with the U.S. National Response Center (NRC) said. The company said September 7 it began shutting down the entire refinery for a 70-day planned turnaround that will tie in units from a $2.2-billion heavy oil upgrade project. Source: http://www.reuters.com/article/2012/09/10/us-refinery-operations-marathon-idUSBRE88905620120910

Food and Agriculture

FDA adds mangoes tied to Salmonella outbreak to import alert list. Mangoes from Mexico linked to a nationwide Salmonella outbreak have been added to the federal import alert list — meaning that districts can detain them without inspection, Food Safety News reported September 14. Mangoes produced by Sinaloa, Mexico-based Agricola Daniella and imported by Splendid Products of Burlingame, California, were recalled August 30 after they were named as the potential source of a Salmonella Braenderup outbreak that has sickened 104 people in 16 States, according to the latest update from the Centers for Disease Control and Prevention. The Food and Drug Administration (FDA) added Daniella brand mangoes to its import alert listings September 12. According to FDA's notice, —Districts may detain, without physical examination, those fresh and raw fresh refrigerated produce from manufacturers, shippers, and/or growers identified in the attachment for this import alert for the microbial contamination indicated. Around 40 U.S. retailers who sold the fruits in stores have recalled the potentially contaminated

product or withdrawn it from shelves, according to information compiled by Food Safety News and eFoodAlert. Source: http://www.foodsafetynews.com/2012/09/mangoes-linked-to-salmonella-outbreak-added-to-fda-import-alert-list/#.UFNFra66TlY

Three deaths counted in Listeria outbreak linked to cheese. A new outbreak of Listeria monocytogenes has killed three people, the federal Centers for Disease Control and Prevention (CDC) said September 11. The deaths are being blamed on cheese imported from Italy. According to CDC, 14 persons were infected with the outbreak strain in 11 States and the District of Columbia. All have been hospitalized. CDC said Listeriosis contributed to at least one death. The CDC report on the outbreak came 24 hours after Long Island-based Forever Cheese recalled one of its imported cheese brands for possible contamination. The number of ill persons identified in each State is as follows: California (1), Colorado (1), District of Columbia (1), Maryland (3), Minnesota (1), Nebraska (1), New Jersey (1), New Mexico (1), New York (1), Ohio (1), Pennsylvania (1), and Virginia (1). Forever Cheese, an importer of products from Italy, Spain, and Portugal, September 10 recalled the Ricotta Salata Frescolina brand from one specific production date for possible Listeria contamination. It also said that the U.S. Food and Drug Administration was investigating. Later September 11, Maryland health officials said three people with Listeria illnesses were being treated in area hospitals. The cheese was sold to distributors for retailers and restaurants in California, Colorado, District of Columbia, Florida, Georgia, Illinois, Indiana, Maine, Maryland, Massachusetts, Montana, New Jersey, New Mexico, New York, Ohio, Oregon, Pennsylvania, Virginia, and Washington between June 20-August 9. Source: http://www.foodsafetynews.com/2012/09/new-listeria-outbreak-already-figures-in-three-deaths/#.UFCXQ666TlY

Corn takes a USDA hit. U.S. farmers will raise slightly less corn than previously expected and a little less soybeans in 2012, according to the U.S. Department of Agriculture (USDA) September 12. In its September Crop Production Report, the USDA dropped the U.S. corn yield from 123.4 bushels per acre in August to 122.8 bushels per acre. U.S. 2012-13 corn production is estimated at 10.72 billion bushels vs. the average analysts' estimate of 10.403 billion bushels and the USDA's previous estimate of 10.779 billion. For soybeans, the USDA estimates a 2012-13 yield of 35.3 bushels per acre vs. the average analysts estimate of 35.5 bu./acre and the USDA's previous estimate of 36.1. The U.S. 2012-13 soybean production estimate is pegged at 2.634 billion bushels vs. the average trade estimate of 2.638 billion bushels and the USDA's previous estimate of 2.692 billion. On 2012-13 U.S. harvested acres, the USDA left those estimates unchanged from a month ago. U.S. corn harvested acreage is pegged at 87.4 million acres and U.S. soybean acreage at 74.6 million. Source: http://www.agriculture.com/news/crops/cn-takes-a-usda-hit_2-ar26314

Farm linked to cantaloupe outbreak now recalling watermelons. The farm in southwestern Indiana whose cantaloupes were pinpointed late in August as the probable source of a Salmonella outbreak that sickened 204 people is now recalling its watermelons because they may be contaminated with a different strain of Salmonella, Food Safety News reported September 10. Chamberlain Farms of Owensville, Indiana, issued a voluntary recall of this growing season's watermelons because they may be contaminated with Salmonella Newport.

An outbreak of Salmonella Typhimurium was linked to the farm August 22 after samples of cantaloupe collected there revealed the presence of the outbreak strain of the bacteria. Missouri-based Schnucks grocery announced the watermelon recall in a press release September 7. Watermelons subject to the recall were sold at Schnucks, Logli, and Hilander stores. Source: http://www.foodsafetynews.com/2012/09/farm-linked-to-cantaloupe-outbreak-now-recalling-watermelons/#.UE3rKK66RnA

Government Sector (including Schools and Universities)

(Louisiana) **Angry over denial for disaster aid, man pulls gun.** A man who allegedly got a fully loaded AR-15 assault rifle from his pickup truck after being turned down for disaster food stamps was jailed in St. John the Baptist Parish, Louisiana, the Associated Press reported September 13. A claims processor in LaPlace told officers that a man became irate after being denied September 11, said a State police spokeswoman. After officers providing security at the location saw him standing next to his truck and handling the weapon, four state troopers, two sheriff's deputies, and six Louisiana National Guard soldiers sneaked up and surrounded him. Investigators also found a handgun and many loaded magazines of ammunition in the truck. The State police spokeswoman said the suspect was booked with terrorizing and aggravated assault. Source: http://www.fox8live.com/story/19529774/man-with-assault-rifle-arrested-at-laplace-dsnap-site

(Vermont) **Vt. police call bomb threat domestic terrorism.** A false report of bombs and a gunman on the way to Montpelier High School September 12 is linked to similar threats last spring and is considered an act of domestic terrorism, Montpelier, Vermont police said. The Montpelier High School was locked down after a phone caller reported shortly before noon that a gunman was en route. The threat included multiple bombs. Police determined the threat was a hoax, similar to other false threats made April 5, and the lockdown was cancelled about 45 minutes later, authorities said. The threats are being made through computer networks involving a host of Internet and landline service providers. In April, the Montpelier Police Department issued a number of subpoenas in the United States and Europe. A suspect or suspects have been identified in Europe. The case is being handled by federal authorities, working with foreign law enforcement in that country, police said. Source: http://www.boston.com/news/education/2012/09/12/vermont-high-school-lockdown-over/CG4wtW6j1jPUFNNTclJXnN/story.html

Protests sweep through Muslim world despite U.S. appeal for calm. The U.S. Secretary of State took strong steps September 13 to distance the U.S. Government from a movie that has sparked protests and violence throughout the Muslim world. In Tripoli, Libya, authorities said a number of people suspected of involvement in an attack on the U.S. Consulate in Benghazi that killed the U.S. Ambassador and three other U.S. officials were detained by security forces. September 13, in Sanaa, Yemen, hundreds of demonstrators converged on a usually sealed-off street in front of the U.S. Embassy for a protest that also turned violent, witnesses said. A State

Department spokeswoman said there had been —a small breach of the compound perimeter but no breach of embassy buildings in Sanaa. She said Yemeni security forces were —in the process of restoring order . Smaller anti-American protests were reported in Iran and Bangladesh. In Dhaka, the Bangladeshi capital, about 100 demonstrators burned an American flag September 13 and chanted slogans. They called for more protests September 14 and said the U.S. Embassy could be the target. Bangladeshi police said security at the embassy was being enhanced. In Tehran, anti-American protesters gathered outside the Swiss Embassy, which represents U.S. interests in Iran. Source: http://www.washingtonpost.com/world/us-embassy-in-yemen-stormed-other-embassies-still-under-siege/2012/09/13/ad65ce7e-fd9b-11e1-a31e-804fccb658f9_story.html

(Georgia; Washington) **5 more charged in Ga. military militia case.** Five more men were charged September 10 in connection with an anti-government militia that authorities say was led by U.S. Army soldiers from Fort Stewart who stockpiled weapons and talked of bombing a Savannah park fountain, poisoning apple crops in the State of Washington, and ultimately overthrowing the U.S. government. A Liberty County, Georgia grand jury indicted the five on charges of illegal gang activity and various counts involving theft, burglary, and auto-break-ins. Those crimes were committed to help fund the militia group, which called itself F.E.A.R., short for Forever Enduring Always Ready, a district attorney said September 11. The new indictments bring to 10 the total number of people charged in connection with the militia group. Source: http://www.militarytimes.com/news/2012/09/ap-five-more-arrested-in-army-militia-091112/

Data breaches expose 94 million records in the government sector. An analysis of government breach data shows that the government sector reported 268 incidents of data breaches from January 1, 2009 to May 31, 2012, which exposed more than 94 million records containing personally identifiable information (PII), according to Rapid7. The research revealed a 50 percent increase in the number of compromises affecting the government sector from 2009 to 2010, as well as a skyrocketing rise in the number of records exposed each year, with the number tripling from 2010 to 2011. Unintended disclosure, the loss/theft of portable devices, physical loss, and hacking continue to be the leading causes of breaches. Analyzing data collected and categorized by the Privacy Rights Clearinghouse Chronology of Data Breaches, Rapid7 discovered additional details regarding breach incidents and government records that were exposed. The number of hacking incidents increased nearly 50 percent year-over-year between 2009 and 2011, with 2012 on pace to more than double that of 2011 entirely. Between January 1, 2012 and May 31, 2012, government agencies reported more hacking incidents than any other type of incident. California (21), District of Columbia (20) and Texas (16) reported the greatest amount of incidents across the country. Source: http://www.net-security.org/secworld.php?id=13553

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

'CRIME' attack abuses SSL/TLS data compression feature to hijack HTTPS sessions. The —CRIME attack announced the week of September 3 exploits the data compression scheme used by the Transport Layer Security (TLS) and SPDY protocols to decrypt user authentication

cookies from HTTPS traffic, one of the attack's creators confirmed September 13. The —CRIME attack was developed by two security researchers who plan to present it the week of September 17 at the Ekoparty security conference in Buenos Aires, Argentina. The week of September 3, the researchers revealed that CRIME abuses an optional feature present in all versions of TLS and Secure Sockets Layer (SSL) — the cryptographic protocols used by HTTPS. However, they declined to name the feature at that time. Source: http://www.computerworld.com/s/article/9231281/_CRIME_attack_abuses_SSL_TLS_data_compression_feature_to_hijack_HTTPS_sessions

874 systems from 33 countries infected with Enfal malware, researchers find. The Enfal malware — best known for its involvement in the LURID targeted attacks — is still causing a lot of damage. Researchers said 874 computers from 33 different countries were infected with a new version of the malicious trojan. An analysis of the command and control (C&C) servers shows that most of the current victims reside in countries such as Vietnam, Russia, and Mongolia. Other affected countries appear to be China (29 infections), Philippines (11 infections), the United States (19 infections), India, and some Middle Eastern States. The main targets seem to be government organizations, military and defense contractors, nuclear and energy sectors, Tibetan communities, and the space and aviation industry, researchers from Trend Micro noted. According to experts, the attacks start with a cleverly designed email that carries malicious attachments. The attachment, a document named Special General Meeting.doc, carries a trojan that exploits a vulnerability in Microsoft Office to drop a backdoor onto the infected computer. Once the trojan is on a system, the malware communicates with its designated C&C server, allowing the cyber criminals to take complete control of the machine. The modifications made to the traditional variant indicate the campaign designers are trying to bypass security mechanisms such as network monitoring and intrusion detection systems. Source: http://news.softpedia.com/news/874-Systems-from-33-Countries-Infected-with-Enfal-Malware-Researchers-Find-292206.shtml

Smartmobe Wi-Fi blabs far too much about us, warn experts. Smartphones leak far more personal information about their users than previously imagined, according to new research. Security researchers at Sensepost were able to track and profile users and their devices by observing the phones' attempts to join Wi-Fi networks. The researchers created their own distributed data interception framework that profiled mobile devices, laptops, and their users in real-time. Smartphones tend to keep a record of Wi-Fi base stations their users previously connected to, and often poll the airwaves to see if a recognized network is within reach. Although this is supposed to make joining wireless networks seamless for users, it also makes it easy for the researchers to link home addresses and other information to individually identifiable devices. Source: http://www.theregister.co.uk/2012/09/14/smartphone_tracking_research/

Blackhole creator releases stealthier exploit kit. The developer of the Blackhole exploit kit has released a new version that makes it more difficult to blacklist URLs pointing to Web sites containing malware. Blackhole version 2.0 was introduced September 11 on the Russian site Malware don't need Coffee. The toolkit, which is popular among cyber criminals, contains many

new features meant to avoid detection from antivirus software. Other improvements include support for Windows 8 and unspecified mobile platforms. Security experts said the most interesting new feature was the ability to generate short-term, random URLs pointing to malicious Web sites or hijacked sites that contain hacker-installed malware. Because the URLs keep changing, it is difficult for search engines, site owners, and security firms to identify malicious pages. Source: http://www.csoonline.com/article/716093/blackhole-creator-releases-stealthier-exploit-kit

NTIA IT security 'significantly' deficient, says OIG. Information technology systems at the National Telecommunications and Information Administration (NTIA) have significant deficiencies, according to a September 7 report from the Commerce Department Office of Inspector General (OIG), FierceGovernmentIT reported September 12. Among the problems are poor security categorizations, weak software and hardware inventory practices, lacking remediation of security problems, mismanaged IT security personnel, and deficient IT security policies and procedures. Report authors found five miscategorized NTIA systems that should have been categorized at a higher security impact level. Without a solid understanding of its assets, NTIA cannot accurately determine risks posed to the system and select appropriate security controls, says the OIG. The agency failed to properly identify all of its hardware and software components. Auditors identified 44 servers and 2 operating systems that were not listed in NTIA's official inventory. They found frequent instances of unsupported and outdated software, and unauthorized movies and games associated with peer-to-peer file sharing. The report recommends that system owners and NTIA officials identify and categorize all —information types that are processed, stored, or transmitted by each system, develop and maintain an accurate inventory, assess and implement IT security controls, and follow NTIA security policies. Source: http://www.fiercegovernmentit.com/story/ntia-it-security-significantly-deficient-says-oig/2012-09-12

Zombie PC herders issue commands from Tor hideout. Security researchers discovered a botnet that uses the Tor anonymizer network to hide its command nodes. The owners of the compromised network of Windows PCs placed their command-and-control server, which uses the common Internet relay chat protocol, as a hidden service inside of the Tor network. This novel approach gives multiple advantages to the zombie PC herders, security firm G-Data explained. Since the server is anonymous, it cannot point towards the botnet owners' identity. Botnet control traffic is encrypted by Tor, so it cannot be blocked by Intrusion Detection Systems monitors. Blocking Tor traffic in general is problematic because there are legitimate uses for the technology. In addition, Tor servers cannot be taken down easily. Source: http://www.theregister.co.uk/2012/09/11/tor_controlled_botnet/

Researchers find flaws in Army-approved FortiGate appliances. Experts from the Vulnerability Lab identified a number of security holes in FortiGate UMT appliances found on the U.S. Army's 2012 Information Assurance Approved Products List (IA APL). The company addressed the vulnerabilities to ensure their customers are protected. Multiple cross-site scripting (XSS) issues were found to affect UTM Firewall appliance applications such as FortiGate-5000 Series, FortiGate-3950 Series, and FortiGate-3810A. Identified in May, the medium-severity flaws could

have been leveraged by a remote attacker to hijack customer and administrator sessions, manipulate Web site context on the client side, and for phishing campaigns. Multiple persistent Web Vulnerabilities also affected the same FortiGate UTM appliance applications. They allowed a remote attacker to persistently inject their own malicious script code to manipulate specific customer and administrator requests. Source: http://news.softpedia.com/news/Researchers-Find-Flaws-In-Army-Approved-FortiGate-Appliances-291459.shtml

SMS phishing attacks skyrocketed last week. In the first week of September, SMS phishing attacks rose 913 percent, making spam the No. 1 text-based threat, said a report from Cloudmark, PC Magazine reported September 10. In a September 7 blog post, Cloudmark's senior security researcher cited a single set of attacks that began September 4 as the culprit for the week's surge. Over the course of 4 days, more than 500 unique phishing scams were sent out by attackers. Each one followed the same general format – —Fwd: Good Afternoon .Attention Required Call.(xxx)xxxxxxx The phone numbers victims were asked to call included area codes from New Jersey, Alabama, Texas, Illinois, California, New York, Rhode Island, Missouri, Florida, Michigan, Georgia, and South Carolina, as well as 866, 877, and 888 toll-free numbers. Cloudmark reported the attackers were phishing for victims' sensitive credentials via Bank of America account suspensions, Macy's credit card collections, and the U.S. Veteran's Administration health services. Source: http://www.pcmag.com/article2/0,2817,2409520,00.asp

Apple device ID leak traced to BlueToad. The source of the database containing 1 million Apple unique device identifiers (UDIDs) published online the week of September 3 by hacking group AntiSec was identified September 10 as BlueToad, an application publisher and analytics provider based in Orlando, Florida. AntiSec said it obtained the database from the FBI, which subsequently disputed that claim. A security researcher working for the Intrepidus Group said he identified BlueToad from patterns in the database itself. In a blog post published September 10, he explained how he sorted the data, identified some 15,000 duplicated UDID numbers, and then linked some of those numbers to BlueToad. He found names in the database shared by BlueToad employees and also discovered passwords from the company that were leaked online. September 5, in response to queries, BlueToad's CIO contacted the security researcher and the company began working on a response. September 10, BlueToad's CEO acknowledged the firm's systems were compromised the week of September 3, and that the list of Apple UDIDs came from its servers. Source: http://www.informationweek.com/security/privacy/apple-device-id-leak-traced-to-bluetoad/240007032

National Monuments and Icons

(California) **Yosemite deer mice being trapped, killed following virus outbreak.** Yosemite National Park in California has begun trapping and killing deer mice whose growing numbers may have helped create the conditions that led to a hantavirus outbreak that has infected eight park visitors and killed three, public health officials said September 11. Yosemite officials in recent weeks have warned 22,000 people who stayed in the park over the summer that they

may have been exposed to the rodent-borne lung disease, which kills over a third of those infected. The Centers for Disease Control and Prevention sounded a worldwide alert and said visitors to the park's Curry Village lodging area between June and August may be at risk. Park officials have closed nearly 100 tent cabins in Curry Village infested with deer mice, which carry the virus. Seven of the eight people confirmed to have been infected are believed to have contracted the virus in the village. Public health officials trapped three times as many deer mice in the park's Tuolumne Meadows the week of September 3 than were caught in a 2008 period, indicating that the deer mice population has grown, said the chief of vector-borne diseases at the State Public Health Department. An infectious disease specialist at the University of California, San Francisco, said the growing deer mice population might help explain the outbreak. Source: http://www.chicagotribune.com/news/sns-rt-us-usa-hantavirus-yosemitebre88b02p-20120911,0,2650132.story

(Idaho; Montana; Oregon) **Wildfires lead to evacuations.** Authorities issued evacuation orders September 9 for Idaho residents in the path of two wildfires where expected strong winds and low humidity could make firefighting difficult. The Lehmi County sheriff issued an evacuation order September 9 for residents along U.S. Highway 93 from Quartz Creek to North Fork threatened by the 408-square-mile Mustang Complex of wildfires on the Montana border that officials fear could spread with high winds. Law enforcement officials September 9 were going door to door notifying residents of about 400 homes. On the other side of the State along the Oregon border, fire officials said evacuations were taking place ahead of the 2.5-square-mile Sheep Fire. The National Weather Service issued a Red Flag Warning September 9 for the region, predicting winds of more than 25 mph combined with low humidity. One firefighter was injured September 8 and had to be taken to a hospital by ambulance. In central Idaho, firefighters had the 228-square-mile Trinity Ridge Fire near Featherville 64 percent contained. To the north, the 232-square-mile Halstead Fire near Stanley was 35 percent contained. Source: http://dnews.com/news_ap/idaho/article_12bccb4b-3d70-5a47-90bc-ceb9a05c7fea.html

Postal and Shipping

(New York) **A 15-year mystery in Syracuse: Who keeps sending these anthrax hoax letters?** The FBI and the U.S. Postal Inspection Service are offering a $10,000 reward for information that leads to the conviction of whoever sent 21 powder-filled letters threatening an anthrax attack from Syracuse, New York, since 1997, the Syracuse Post-Standard reported September 9. The FBI has evidence that for the past 15 years someone in Syracuse has been inducing panic among office workers with the powder-filled letters. The pattern is the same: A letter arrives with a mound of white powder inside, claiming it is anthrax. The letters also carry clues about the sender, including his penchant for the writings of a long-dead science fiction writer. Then the terrorist disappears for months, even years. Ten of the letters went to a high school, a college, a business, and a Congresswoman's office in the Syracuse area. The other 11 went to military and police associations, nonprofit groups, government officials, private businesses, and TV celebrities all across the eastern United States, according to the FBI. The mailings started long before the nationwide anthrax scare that followed the September 11, 2001, terrorist attacks. The letters were sent from Syracuse in 1997, 1999, 2002, 2010, 2011, and 2012.

Source:
http://www.syracuse.com/news/index.ssf/2012/09/fbi_tracks_15_years_of_white_p.html#incart_river_default

PUBLIC HEALTH

Outbreak study details waning protection from pertussis vaccine. The Center for Infectious Disease Research and Policy reported September 13 that a detailed look at California children during the State's large pertussis outbreak in 2010 revealed that protection from the diphtheria, tetanus, and pertussis (DTaP) vaccine wanes 5 years after children receive their last dose, which could be fueling outbreaks. The findings come on the heels of a warning earlier this summer from the Centers for Disease Control and Prevention (CDC). The agency, along with State health department partners, found an unusual illness spike in 13- and 14-year-olds in Washington, which also raised the possibility of waning pertussis (whooping cough) vaccine protection. The United States was headed toward its worst pertussis year in decades, CDC officials said in July, and two States — Washington and Colorado — have declared epidemics. Source: http://www.cidrap.umn.edu/cidrap/content/other/news/sep1312pertussis.html

Dirty bomb threat lurks in U.S. hospitals, fed study warns. The Government Accountability Office (GAO) released a report September 11 saying that hospitals have been negligent in securing the radioactive materials they use to treat cancer patients, potentially putting the materials in the hands of terrorists who could use them to make a dirty bomb. The GAO warned Congress about lapses in hospitals, many of which routinely use equipment containing radioactive materials. Nearly four out of five hospitals across the country have failed to put in place safeguards to secure radiological material that could be used in a dirty bomb, according to the report, which identifies more than 1,500 hospitals as having high-risk radiological sources. According to the report, the National Nuclear Security Administration spent $105 million to complete security upgrades at 321 of more than 1,500 hospitals and medical facilities that were identified as having high-risk radiological sources. The upgrades included security cameras, iris scanners, motion detectors, and tamper alarms. But these upgrades are not expected to be completed until 2025, so many hospitals and medical centers remain vulnerable, the GAO said. The Nuclear Regulatory Commission challenged the GAO's findings, saying that the agency and its partners are vigilant about protecting hospitals and medical facilities, and had developed additional voluntary layers of security to do so. The American Hospital Association said it was reviewing the GAO's recommendations. Source: http://abcnews.go.com/US/negligent-security-radioactive-material-hospitals-terrorism-risk-gao/story?id=17207135#.UE9owrJlRjV

(Florida) **3 carjack truck carrying prescription drugs.** Police were searching for three armed robbers who carjacked a truck during a delivery of pharmaceuticals September 7 in Miami Beach, Florida. According to police, a truck was scheduled to drop off merchandise at a pharmacy when the driver was held up at gunpoint and carjacked. After pulling the driver out and pointing a gun at him, authorities said, the three men jumped in the truck and fled. Police were looking for a white cargo van with windows in the back. Source:

http://www.wsvn.com/news/articles/local/21008473183262/3-carjack-truck-carrying-pharmaceutical-drugs/

Transportation

Nothing Significant to Report

Water and Dams

EPA proposes adding groundwater plume in Salt Lake City to Superfund site list. The U.S. Environmental Protection Agency (EPA), with support from Utah Department of Environmental Quality, Salt Lake Valley Health Department, and Salt Lake City, announced a proposal September 14 to add the PCE Plume, in Salt Lake City to the National Priorities List (NPL) of Superfund sites. The listing will make the site eligible for comprehensive assessment and cleanup through the Superfund process and mandate the availability of federal funds for cleanup. Sampling and investigations by the State and EPA indicate groundwater in the area is contaminated with tetrachloroethylene, commonly known as PCE. The groundwater plume, first discovered in 1990 during routine sampling of the Mount Olivet Cemetery irrigation well, contains levels of PCE above federal drinking water standards. In 2010, water samples taken by the city from natural springs fed by groundwater in the area also indicated the presence of PCE. Left unaddressed, the PCE plume is likely to grow in size, further endangering public water supplies. EPA proposed to add eight sites nationally to the NPL September 14. Source: http://yosemite.epa.gov/opa/admpress.nsf/0/da97fdf3eab1310585257a7900516ff9?OpenDocument

(California) **Riverside County declares state of emergency.** Riverside County, California, declared a state of emergency after severe flooding forced hundreds of people from their homes September 12 so they can apply for state and federal money to help with cleanup and rebuilding costs. Eleven homes were without power and people relied on bottled water in Duroville, a mobile home park. County officials said they plan to ship water to the community. Heavy rains sent water rushing into low-lying areas. Much of the water drained or flowed away from Duroville toward the nearby Salton Sea, but troubled spots remained. One of the two water pumps at the mobile home park damaged by the flooding was repaired and authorities checked to see if the sewer system was compromised. Source: http://www.mercurynews.com/breaking-news/ci_21533469/riverside-county-declares-state-emergency

Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of

Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168